



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/782,751

02/23/2004

Nicolas Popp

12832/100002

6185

23838 7590 10/17/2007  
KENYON & KENYON LLP  
1500 K STREET N.W.  
SUITE 700  
WASHINGTON, DC 20005

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT

PAPER NUMBER

2134

MAIL DATE

DELIVERY MODE

10/17/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/782,751

Applicant(s)

POPP, NICOLAS

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 23 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1 and 2 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 2 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 February 2004 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 9/27/2005.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. The IDS of 9/27/2005 was received and considered.
2. Claims 1-2 are pending.

***Information Disclosure Statement***

3. The information disclosure statement (IDS) submitted on 9/27/2005 was considered by the examiner. However, the IDS states "1 of 2" in the sheet listing at the top. A copy of the PCT search report for PCT US05/05482 was also submitted, but not listed on an IDS. Applicant's representative, Gary Morris, was contacted at 202-434-8195 on 10/4/2007 and a messages was left requesting clarification as to whether a second page was to be included in the IDS, but no call was returned as of 10/9/2007. Accordingly, the examiner has considered sheet 1 of 2 to be a typographical error and has replaced this with sheet 1 of 1. The PCT search report has also been considered, even though it does not appear on the 1449 of 9/27/2005. Applicant is requested to provide clarification of this issue in the response to this action; if applicant intended to include the above-mentioned search report on the 1449, applicant is requested to submit an additional information disclosure statement listing the search report to clarify the record.

***Drawings***

4. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because Figs. 2-3 are handwritten and difficult to read. Applicant is advised to employ the services of a competent patent draftsman outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 101***

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-2 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. Regarding claims 1-2, the claims are directed to a digital certificate (data structure) which is non-functional descriptive content, not falling within one of the statutory classes of invention. Further, the claimed digital certificate, even if it were tangibly embodied on a medium, would not meet the requirement under 35 U.S.C. §101 because the non-functional data structure would not necessarily have a functional interrelationship with the medium.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 6,088,722 to Herz et al. (Herz).

Regarding claim 1, Herz discloses a digital certificate (E(N,P), which is seed N encrypted using public key P, Fig. 7, ##702, 704, 706, i.e. public key P is certifying seed N) including a secret (seed N) encrypted by a public key associated with a device (set top's public key, Fig. 7, #704 & col. 46, lines 7-

Art Unit: 2134

10), wherein the secret (seed N) is used by the device (set top) to generate a plurality of One Time Passwords (pseudo random numbers, Fig. 7, ##714-716, 718 & col. 45, lines 38-62).

***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 1-2 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication 2002/0144119 to **Benantar** in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**).

Regarding claim 1, Benantar discloses a digital certificate (attribute certificate, ¶103) including a secret (authentication data, ¶103, where authentication data is a password, ¶96) encrypted (authentication data is encrypted, ¶101) by a public key (user's public key, ¶101) associated with a device (client the user is using, ¶100), but lacks wherein the secret is used by the device (client) to generate a plurality of One Time Passwords. However, Menezes teaches a one-time password scheme where a claimant A has a shared password P with the system verifier B, to which A sends the data pair (r, H(r,P)). The verifier then computes the hash of the received value r and its local copy of P and declares acceptance if this matches the received hash value, where r should be a sequence number, time-stamp or other parameter which can be easily guaranteed to be accepted only once (p. 397, 10.8 Note). One-time password schemes are useful because they are safe from passive adversaries who eavesdrop and later attempt impersonation (p. 396, first two lines). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Benantar's client, such that

Art Unit: 2134

rather than sending the plain password to the target application (as in ¶108), the client hashes the password with a sequence number, time-stamp or other parameter which can be easily guaranteed to be accepted only once and then sends the result to the target application. One of ordinary skill in the art would have been motivated to perform such a modification to make the authentication procedure safe from passive adversaries who eavesdrop and later attempt impersonation, as taught by Menezes (pp. 396-397).

Regarding claim 2, Benantar, as modified above, discloses wherein the digital certificate (attribute certificate, ¶103) is a PKI certificate (¶91 & ¶111).

### ***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

b. U.S. Patent Application Publication 2002/0199119 to Dunnion et al. is cited for teaching time-varying authentication (OTP, ¶83).

c. WIPO publication WO 03/001736 A1 is cited for teaching authentication using one-time passwords and certificates.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 11, 2007  
Michael J. Simitoski  
/ Michael J. Simitoski/